IN THE CLAIMS

1. (Currently amended) A system for network security comprising:

a first network device having a first encryption key, the first encryption key including a first base key and a key extension in addition to the first base key~~;~~, the key extension being based on a hash function of an internal key and a network device identifier;

a second network device having the first encryption key and a second encryption key, the second encryption key including a second base key, wherein the second network device is capable of communicating with the first network device using security determined by the first encryption key; and

a third network device having the second encryption key, wherein the third network device is capable of communicating with the second network device using security determined by the second encryption key~~;~~ ~~and~~

wherein the first encryption key is used to encrypt and decrypt communications between the first and second network devices, and the second encryption key is used to encrypt and decrypt communications between the second and third network devices~~;~~; and

wherein the security determined by the first encryption key is stronger than the security determined by the second encryption key.

2. (Previously presented) The system of claim 1 wherein the first encryption key has a bit length that is longer than a bit length of the second encryption key.

3. (Original) The system of claim 2 wherein the first encryption key has a length of

greater than a threshold number of bits, and the second encryption key has a length of no greater than the threshold number of bits.

4. (Original) The system of claim 3 wherein the threshold is 64 bits.

5. (Canceled).

6. (Canceled).

7. (Canceled).

8. (Original) The system of claim 1 wherein the first network device is located in a first jurisdiction, and the second network device is located in a second jurisdiction outside of the first jurisdiction.

9. (Original) The system of claim 1 wherein the first and second base keys are each based on at least a pre-shared key and a computed private key.

10. (Original) The system of claim 9 wherein the computed private key is a Diffie-Hellman key.

11. (Canceled).

12. (Currently amended) The system of claim 1 ~~11~~ wherein the network device identifier is a software serial number.

13. (Currently amended) A system for network security comprising:

a first network device having a first encryption key, the first encryption key including a first base key and a first key extension in addition to the first base key, and a second encryption key, the second encryption key including a second base key and a second key extension in addition to the second base key~~;~~, each of the first and second key extensions being based on a hash function of an internal key and a network device identifier;

a second network device having the first encryption key and a third encryption key, the third encryption key including a third base key, wherein the second network device is capable of communicating with the first network device using security determined by the first encryption key; and

a third network device having the second encryption key and the third encryption key, the third network device being capable of communicating with the first network device using security determined by the second encryption key, and the third network device also being capable of communicating with the second network device using security determined by the third encryption key~~;~~;

wherein the first encryption key is used to encrypt and decrypt communications between the first and second network devices, the second encryption key is used to encrypt and decrypt communications between the first and third network devices, and the third encryption key is used to encrypt and decrypt communications between the second and third network devices~~;~~ ~~and~~

wherein the security determined by the first encryption key is stronger than the security

determined by the third encryption key;; and

wherein the security determined by the second encryption key is stronger than the security determined by the third encryption key.

14. (Previously presented) The system of claim 13 wherein the first and second encryption keys each have a bit length that is longer than a bit length of the third encryption key.

15. (Original) The system of claim 14 wherein the first and second encryption keys each have a length of greater than a threshold number of bits, and the third encryption key has a length of no greater than the threshold number of bits.

16. (Original) The system of claim 15 wherein the threshold is 64 bits.

17. (Canceled).

18. (Canceled).

19. (Canceled).

20. (Original) The system of claim 13 wherein the first network device is located in a first jurisdiction, and the second network device is located in a second jurisdiction outside of the first jurisdiction.

21. (Original) The system of claim 13 wherein the first, second, and third base keys are each based on at least a pre-shared key and a computed private key.

22. (Original) The system of claim 21 wherein the computed private key is a Diffie-Hellman key.

23. (Canceled).

24. (Currently amended) The system of claim 13 ~~23~~ wherein the network device identifier is a software serial number.

25. (Currently amended) A method for network security comprising the steps of:

providing a first network device, a second network device, and a third network device;

establishing a first secure communication between the first and second network devices based on a first encryption key, the first encryption key having a base key and a key extension in addition to the base key;

establishing a second secure communication between the second and third network devices based on a second encryption key; ~~and~~

basing each of the base key and the second encryption key on at least a pre-shared key and a computed private key;

basing the key extension on a hash function of an internal key and a network device identifier; and

using a stronger security for the first secure communication than the second secure

communication;

wherein using the stronger security for the first secure communication than the second secure communication comprises using security determined by the first encryption key for the first secure communication, the first encryption key being used to encrypt and decrypt communications between the first and second network devices, and using security determined by the second encryption key for the second secure communication, the second key being used to encrypt and decrypt communications between the second and third network devices; and

wherein the security determined by the first encryption key is stronger than the security determined by the second encryption key.

26. (Previously presented) The method of claim 25 wherein the second encryption key is identical to the base key.

27. (Previously presented) The method of claim 25 further comprising the steps of using a length of greater than a threshold number of bits for the first encryption key, and using a length of no greater than the threshold number of bits for the second encryption key.

28. (Previously presented) The method of claim 27 wherein the threshold is 64 bits.

29. (Canceled).

30. (Previously presented) A computer readable medium having stored therein instructions for causing at least one central processing unit to execute the method of claim 25.

31. (Currently amended) A method for network security comprising the steps of:

providing a first network device, a second network device, and a third network device;

negotiating a first secure communication between the first and second network devices based on a first authentication key, the first authentication key having a base key and a key extension in addition to the base key;

deriving a first encryption key from the negotiation of the first secure communication;

negotiating a second secure communication between the second and third network devices based on a second authentication key;

deriving a second encryption key from the negotiation of the second secure communication; ~~and~~

basing each of the base key and the second authentication key on at least a pre-shared key and a computed private key;

basing the key extension on a hash function of an internal key and a network device identifier; and

using a stronger security for the first secure communication than the second secure communication~~;~~;

wherein using the stronger security for the first secure communication than the second secure communication comprises using security determined by the first encryption key for the first secure communication, the first encryption key being used to encrypt and decrypt communications between the first and second network devices, and using security determined by the second encryption key for the second secure communication, the second encryption key being used to encrypt and decrypt communications between the second and third network

devices;; and

wherein the security determined by the first encryption key is stronger than the security determined by the second encryption key.

32. (Original) The method of claim 31 wherein the second authentication key is identical to the base key.

33. (Previously presented) The method of claim 31 further comprising the steps of using a length of greater than a threshold number of bits for the first encryption key and using a length of no greater than the threshold number of bits for the second encryption key.

34. (Original) The method of claim 33 wherein the threshold is 64 bits.

35. (Canceled).

36. (Original) A computer readable medium having stored therein instructions for causing at least one central processing unit to execute the method of claim 31.

37. (Currently amended) A system for network security comprising:

a first network device having a first authentication key, the first authentication key including a first base key and a key extension in addition to the first base key, the key extension being based on a hash function of an internal key and a network device identifier;

a second network device having the first authentication key and a second authentication key, the second authentication key including a second base key, wherein the first and second devices are capable of using the first authentication key to negotiate a first encryption key so as to communicate using security determined by the first encryption key; and

a third network device having the second authentication key, wherein the second and third network devices are capable of using the second authentication key to negotiate a second encryption key so as to communicate using security determined by the second encryption key;;

wherein the first encryption key is used to encrypt and decrypt communications between the first and second network devices, and the second encryption key is used to encrypt and decrypt communications between the second and third network devices;; and

wherein the security determined by the first encryption key is stronger than the security determined by the second encryption key.

38. (Previously presented) The system of claim 37 wherein the first encryption key has a length of greater than a threshold number of bits, and the second encryption key has a length of no greater than a threshold number of bits.

39. (Previously presented) The system of claim 38 wherein the threshold is 64 bits.

40. (Currently amended) A system for network security comprising:

a first network device having a first authentication key, the first authentication key including a first base key and a first key extension in addition to the first base key, and a second authentication key, the second authentication key including a second base key and a second key

extension in addition to the second base key, each of the first and second key extensions being based on a hash function of an internal key and a network device identifier;

a second network device having the first authentication key and a third authentication key, the third authentication key including a third base key, wherein the first and second network devices are capable of using the first authentication key to negotiate a first encryption key so as to communicate using security determined by the first encryption key; and

a third network device having the second authentication key and the third authentication key, the first and third network devices being capable of using the second authentication key to negotiate a second encryption key so as to communicate using security determined by the second encryption key, and the second and third network devices being capable of using the third authentication key to negotiate a third encryption key so as to communicate using security determined by the third encryption key;

wherein the first encryption key is used to encrypt and decrypt communications between the first and second network devices, the second encryption key is used to encrypt and decrypt communications between the first and third network devices, and the third encryption key is used to encrypt and decrypt communication between the second and third network devices, and

wherein the security determined by the first encryption key is stronger than the security determined by the third encryption key; and

wherein the security determined by the second encryption key is stronger than security determined by the third encryption key.

41. (Previously presented) The system of claim 40 wherein the first and second encryption keys each have a length of greater than a threshold number of bits, and the third encryption key has a length of no greater than a threshold number of bits.

42. (Previously presented) The system of claim 41 wherein the threshold is 64 bits.